CONSUMER ADVISORY

June 2014 **By Attorney General Tom Miller**

The Drive to Destroy

Removing data from computer hard drives, storage devices & wireless phones

While the word "delete" means "remove," did you know that deleting files from your computer's storage device doesn't generally remove them? That's important, because computer storage devices often store very sensitive data, such as passwords, financial information and personal files. If you're selling, donating or disposing of a computer or data storage device, or you're simply replacing a hard drive, don't take chances by allowing others to retrieve your personal data.

Computers, Tablets & Hard Drives

Deleting a file or reformatting a computer or tablet's hard drive simply removes its indexing information, or road map, that the device uses to locate the raw data. Since the data still exists, someone using data recovery software – some of which is available for free – can retrieve deleted files. The only way to ensure that you have permanently erased data from a hard drive is to thoroughly overwrite it. Wiping a hard drive (using a "thorough" over a "quick" setting, which will repeatedly overwrite a hard drive) will irretrievably erase everything. It is better to overwrite or wipe a hard drive several times (ideally three to seven times), as opposed to once.

You can purchase software to wipe a hard drive or thoroughly erase selected files, and there is also free software that you can download. Before choosing software, be sure to understand its features, including its level of overwriting. And chances are that free software won't include technical support beyond information posted on a website.

Physically destroying a hard drive is also an option. A common method is to drill four holes through the entire drive, shred it, or pry the internal hard drive platters so they cannot function. Physical destruction is best left to a professional.

Federal law requires that businesses follow data security and disposal requirements in removing business-related personal and financial information from computer equipment.

Flash Drives, DVDs & CDs

A flash drive is another type of storage device. Like with hard drives, deleting a file from a flash drive does not ensure that the data has been permanently erased. To permanently remove data from a flash drive or thoroughly wipe the flash drive, use software that is designed for that purpose. For DVDs and CDs, cut or shred them (many heavy duty paper shredders will work). You can wipe rewritable discs, and there is software you can use to ensure you overwrite them securely.

Wireless Phones

Your wireless phone likely contains sensitive information, such as contacts, voice and text messages, and other personal data. A smartphone may be a gateway into personal and work email accounts, or other accounts that enable the user to make purchases. When trading, selling, donating or disposing of your smartphone, make sure your data doesn't go with it.

Most phones use removable Subscriber Identity Module (SIM) cards to store contact data, and many phones also utilize separate secure digital (SD) cards to store photos, video and other files. Remove the cards and then initiate a factory reset to wipe other sensitive data. As these procedures vary by model, consult the user manual, manufacturer's website, or your wireless carrier for more information. Be sure to check your phone to ensure your contact information and other personal information has been erased. Ask your wireless carrier about transferring your SIM and SD cards to another phone.

Dispose of Electronics Properly

Check with your local waste authority on properly disposing of electronics, as most computer equipment contains hazardous materials that should not go to a landfill. Some businesses collect, refurbish or recycle certain electronic items.